De beveiligingsplicht in wet- en regelgeving

Nouwt, J.

Published in:
NEN 7510

Publication date:
2005

Sjaak Nouwt

De beveiligingsplicht in wet- en regelgeving

Sjaak Nouwt is werkzaam bij het Centrum voor Recht, Technologie en Samenleving (TILT) van de Universiteit van Tilburg.

Inleiding

De beveiliging van persoonsgegevens is één van de algemene privacybeginselen zoals die aan het begin van de jaren '80 al zijn geformuleerd door de Organisatie voor Economische Samenwerking en Ontwikkeling in de OECD *Guidelines on the Protection of Privacy and Transborder Flow of Personal Data* (Parijs 1981) en door de Raad van Europa in het *Verdrag tot bescherming van personen met betrekking tot de geautoma-tiseerde verwerking van persoons-gegevens* (Straatsburg 28 januari 1981).
De algemene privacybeginselen uit deze internationale documenten vormen nog steeds de grondslag voor de huidige bescherming van persoonsgegevens, ook wel informationele privacy genoemd, in ons land. Het Nederlandse stelsel van privacybescherming bestaat uit een nadere uitwerking van deze beginselen. Met de maatregelen op nationaal niveau is invulling gegeven aan de doelen die zijn neergelegd in de afzonderlijke privacybeginselen.
Het beveiligingsbeginsel houdt in dat persoonsgegevens moeten worden beschermd met redelijke beveiligingsmaatregelen tegen verlies van of ongeoorloofde toegang tot gegevens alsmede tegen ongeoorloofde vernietiging, gebruik, verandering of uitlekken daarvan. Bij het treffen van maatregelen ter beveiliging van persoonsgegevens moet onder andere worden gelet op de mate van gevoeligheid van de gegevens, de mate waarin de toegang tot de gegevens binnen een organisatie beperkt dient te worden en de behoefte aan het kunnen bewaren van de gegevens gedurende langere tijd. Beveiligingsmaatregelen moeten zijn gebaseerd op gangbare methoden en technieken van gegevensbeveiliging.
Wat gangbaar is hangt af van de stand van de techniek, die voortschrijdt met de tijd. De maatregelen worden getroffen om persoonsgegevens te beschermen tegen:

a verlies en onbedoeld wissen van gegevens;
b onbevoegde toegang tot gegevens;
c de ongeoorloofde vernietiging van gegevens, waaronder begrepen het onbevoegd vernietigen en ontvreemden van opslagmedia;
d onbevoegd gebruik van persoonsgegevens inclusief het ongeautoriseerd kopiëren van gegevens;
e ongeoorloofde wijziging of vervalsing van gegevens, met inbegrip van het ongeautoriseerd invoeren van gegevens: iemand kan bevoegd toegang hebben tot bepaalde gegevens teneinde deze te raadplegen, hetgeen echter niet automatisch het recht inhoudt deze gegevens te wijzigen of nieuwe gegevens aan het bestand toe te voegen;
f ongeoorloofde verspreiding of openbaarmaking.

Beveiligingsmaatregelen kunnen worden getroffen op het niveau van (a) fysieke beveiliging: gesloten deuren of identificatie-

De DBC's maken de zorgbedrijven tot ondernemingen die opereren in een markt die de Elseviertest transparant maakt. Degenen met een zwakke informatievoorziening zullen het niet redden. Het is up –met NEN 7510– or out.

Jaap van de Wel, Comfort-IA

pasjes, (b) organisatorische beveiliging: bevoegdhedenregeling met betrekking tot de toegang tot gegevens of (c) informationele beveiliging: encryptie of elektronisch toezicht op ongebruikelijke activiteiten. Tot de organisatorische maatregelen wordt ook gerekend de geheimhoudingsplicht voor het gegevensverwerkend personeel.
De maatregelen die voortvloeien uit dit beginsel vertonen enige overlap met de toegangs- en verstrekkingenproblematiek: wie mogen toegang hebben tot patiëntengegevens en aan wie mogen ze worden verstrekt? Daarvoor bestaan aanknopingspunten in wet- en regelgeving.

Wet bescherming persoonsgegevens

Ter implementatie van de richtlijn van de EU ter bescherming van persoonsgegevens[1] bevat artikel 13 van de Wet bescherming persoons gegevens (WBP) de volgende beveiligingsplicht:

'De verantwoordelijke legt passende technische en organisatorische maatregelen ten uitvoer om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. Deze maatregelen garanderen, rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau gelet op de risico's die de verwerking en de aard van te beschermen gegevens met zich meebrengen. De maatregelen zijn er mede op gericht onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen.'

Uiteraard zal eerst moeten worden vastgesteld of de WBP van toepassing is. Dat houdt in dat vast moet staan dat persoonsgegevens worden verwerkt op een geheel of gedeeltelijk geautomatiseerde wijze. Als dat het geval is, dan is de WBP van toepassing. Dan is voorts van belang dat voldoende duidelijk is wie de 'verantwoordelijke' is voor de gegevensverwerking. Dat is de persoon of organisatie die het doel en de mid-delen van de gegevensverwerking bepaalt. Een ziekenhuis zal bijvoorbeeld 'verantwoordelijke' zijn voor het ziekenhuisinformatiesysteem. Bij samenwerkingsverbanden is het soms lastiger om vast te stellen wie 'de verantwoordelijke' is. Dat is echter wel belangrijk, mede met het oog op de vraag wie verantwoordelijk is of zijn voor het treffen van voldoende beveiligingsmaatregelen.

Op grond van artikel 14 WBP geldt de beveiligingsplicht ook voor de eventuele bewerker van de persoonsgegevens. Een bewerker is degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt, zonder rechtstreeks aan diens gezag te zijn onderworpen. Het gaat dan bijvoorbeeld om een bedrijf waaraan de geautomatiseerde verwerking is uitbesteed.
Wanneer een verantwoordelijke (bijvoorbeeld een ziekenhuis) gebruik maakt van de diensten van een bewerker, dan heeft deze verantwoordelijke de zorgplicht dat de bewerker de persoonsgegevens uitsluitend verwerkt in opdracht van de verantwoordelijke en dat de bewerker de beveiligingsverplichtingen nakomt die op grond van art. 13 WBP op de verantwoordelijke rusten. Daartoe zal de verantwoordelijke een bewerkersovereenkomst, bijvoorbeeld in de vorm van een Service Level Agreement (SLA) met de bewerker moeten aangaan waarin aan de bewerker deze en andere verplichtingen kunnen worden opgelegd.

Volgens minister Hoogervorst bevat NEN norm 7510 goede aanknopingspunten om concreet invulling te geven aan de plicht van art. 13 WBP tot het treffen van passende technische en organisatorische maatregelen: '*Een passend beveiligingsniveau is een vereiste om gegevens uit te wisselen. Als uitgangspunt daarvoor zal de recent vastgestelde norm voor informatiebeveiliging in de zorg gaan gelden, NEN 7510.'*[2]

Behalve in NEN norm 7510 kan ook in het onderzoeksrapport van het College bescherming persoonsgegevens over beveiliging van persoonsgegevens een praktisch hulpmiddel worden gevonden voor de concretisering van de algemene beveiligingsplicht.[3]

Wet geneeskundige behandelingsovereenkomst

In het geval persoonsgegevens over iemands gezondheid worden gebruikt in de context van een geneeskundige behandeling, zijn de regels uit het Burgerlijk Wetboek (waarin de Wet geneeskundige behandelingsovereenkomst WGBO is opgenomen) van toepassing. De WGBO kent een geheimhoudingsplicht voor hulpverleners.[4] Die geheimhoudingsplicht is mede van belang voor de beveiliging van patiëntgegevens. Met het oog op de naleving van de geheimhoudingsplicht moet een hulpverlener er dus voor zorgen dat de

patiëntengegevens voldoende beveiligd zijn.
De hoofdregel voor de omgang met patiëntgegevens vinden we in art. 7:457, eerste en tweede lid, BW: de hulpverlener (arts of instelling) moet er voor zorgen dat zonder toestemming van de patiënt geen inlichtingen over de patiënt, dan wel inzage in of afschrift van diens bescheiden aan anderen wordt verstrekt. Onder 'anderen' wordt niet verstaan: 'degenen die rechtstreeks betrokken zijn bij de uitvoering van de behandelingsovereenkomst en degene die optreedt als vervanger van de hulpverlener, voorzover de verstrekking noodzakelijk is voor de door hen in dat kader te verrichten werkzaamheden'. Aan deze personen mogen dus wel inlichtingen worden verstrekt zonder toestemming van de patiënt.
Een hulpverlener moet bij al zijn werkzaamheden de 'zorg van een goed hulpverlener' in acht nemen. Deze algemene norm fungeert vooral als vangnet voor gevallen waarin de wet niet duidelijk is. Naast 'de zorg van een goed hulpverlener', moet de hulpverlener ook altijd handelen in overeenstemming met de op hem rustende verantwoordelijkheid die voortvloeit uit de voor hulpverleners geldende professionele standaard (art. 7:453 BW). Hiermee wordt mede gedoeld op de normen, regels en ervaringen uit de beroepsgroep. De professionele standaard omvat het geheel van regels en normen waarmee de hulpverlener bij het uitoefenen van zijn werkzaamheden rekening behoort te houden. Algemeen wordt aange-nomen dat de professionele standaard niet alleen de vaktechnische aspecten van de medische beroepsuitoefening omvat, maar ook de normen die gelden voor de relatie met de patiënt en maatschappelijke zorgvuldigheidseisen. Daartoe behoren, naast de wettelijke normen, ook normen en regels uit de beroepsgroep, zoals de 'Gedragsregels voor artsen' en de 'Richtlijnen inzake het omgaan met medische gegevens' van de KNMG. Het is aannemelijk dat ook NEN Norm 7510 tot de professionele standaard moet worden gerekend. Anders dan de norm 'de zorg van een goed hulpverlener', die ook geldt voor zorginstellingen, geldt de norm 'professionele standaard' enkel voor de individuele hulpverlener (arts, psycholoog, verpleegkundige, etc.).
Onderdeel van de beveiliging tegen onrechtmatige verwerking, in het bijzonder de onrechtmatige toegang tot persoonsgegevens, is het regelen van de toegang tot patiëntengegevens. Daarvoor is van belang dat een toegangsregeling wordt opgesteld. De verantwoordelijke voor de gegevensverwerking dient vervolgens met een zekere regelmaat na te lopen of degenen die op basis daarvan toegang hebben, die toegangsmogelijkheid op een bepaald moment nog steeds nodig hebben. Een voorbeeld van een toegangsregeling is te vinden in het rapport over de implementatie van de WGBO.[5]

Wet BIG en Kwaliteitswet Zorginstellingen

Artikel 2 van de Kwaliteitswet zorginstellingen (KWZ) en art. 40 van de Wet beroepen in de individuele gezondheidszorg (Wet BIG) schrijven voor dat hulpverleners 'verantwoorde zorg' aan patiënten moeten aanbieden. 'Verantwoorde zorg' is zorg van inhoudelijk goed niveau die in ieder geval doeltreffend, doelmatig en patiëntgericht wordt verleend en die voldoet aan de behoefte van de patiënt.
De KWZ geldt voor instellingen die zorg verlenen. Een instelling is een organisatorisch verband waarbinnen zorg wordt verleend.

NEN 7510 geeft mij de meetlat die ik als functionaris voor de gegevensbescherming nodig heb. In combinatie met de mplementatievoorschriften heb ik nu een passend toetsingskader voor onze informatievoorziening.

Luuc Posthumus, AMC

Informatiebeveiliging heeft niet zozeer te maken met instrumenten zoals virusscanners en wachtwoorden. Deze zichtbare kenmerken van beveiliging zijn afhankelijk van de stand der techniek op een bepaald moment en worden in de loop der tijd vervangen door andere technologie. Effectieve informatiebeveiliging valt of staat echter met het bewustzijn dat veilig werken zich ook moet uiten in het op verantwoorde wijze met informatie omgaan.

Hans van Vlaanderen, SIVZ

Deze omschrijving dekt in beginsel alle intra- en extramurale voorzieningen voor algemene en geestelijke gezondheidszorg, ouderenzorg en gehandicaptenzorg. Daarnaast geldt ook een samenwerkingsverband van enkele beroepsbeoefenaren in een groepspraktijk als een instelling in de zin van deze wet.
De Wet BIG bevat de pendant van de verplichting om 'verantwoorde zorg' te verlenen voor individuele hulpverleners die als 'echte solisten' kunnen worden beschouwd. Voor hen houdt deze norm in dat zij hun beroepsuitoefening in personeel en materieel opzicht zodanig dienen te organiseren dat dit leidt of redelijkerwijze moet leiden tot 'verantwoorde zorg'.
Een goede beveiliging van patiëntgegevens tegen onbevoegde kennisneming behoort ook tot de plicht om 'verantwoorde zorg' te leveren.

Slot

Beveiliging van persoonsgegevens is een al jarenlang op nationaal en internationaal niveau onbetwist privacybeginsel. Als zodanig is de algemene wettelijke verplichting tot beveiliging van persoonsgegevens te vinden in de WBP. Daarnaast valt de beveiligingsplicht ook uit andere bestaande normen in de gezondheidswetgeving af te leiden. Dat geldt bijvoorbeeld voor de WGBO (geheimhoudingsplicht, zorg van een goed hulpverlener, de professionele standaard), de KWZ en de Wet BIG (verantwoorde zorg).
Deze algemene normen bieden echter weinig houvast voor de concrete invulling van de wettelijke beveiligingsplicht in de praktijk. Die houvast kan wel worden gevonden in NEN norm 7510. De minister van VWS is dan ook terecht van mening dat NEN Norm 7510 het uitgangspunt moet zijn voor de naleving van de wettelijke beveiligingsplicht

1 Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens. *Publicatieblad* Nr. L 281 van 23/11/1995 0blz. 003-0050.

2 *Kamerstukken II*, 2004/05, 29 800 XVI, nr. 2, p. 134

3 Blarkom, G.W. van , Borking, drs. J.J., *Beveiliging van persoonsgegevens.*

Registratiekamer, april 2001. Achtergrondstudies en Verkenningen 23. www.cbpweb.nl

4 Evenals bijvoorbeeld art. 9, lid 4, art. 12, lid 2 en art. 21, lid 2, WBP en art. 88 Wet Beroepen in de individuele gezondheidszorg (Wet BIG)

5 J.M. Witmer, R.P. de Roode (eindred.), V*an wet naar praktijk. Implementatie van de WGBO. Deel 4: Toegang tot patiëntengegevens*. Utrecht: KNMG juni 2004, bijlage 2. www.knmg.nl.wgbo